

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A computer implemented method of detecting scanning attacks, comprises:
 3. adding host-pair connection records to a first data structure stored on a computer readable medium when a host accesses another host during a first update period;
 6. determining the number of new host pairs added to the first data structure over the first update period;
 8. aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update period; wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;
 13. determining the number of new host pairs added to the second data structure over the second update period; and
 15. indicating a host as a scanner when at least one of the following conditions is true:
 17. (1) the host appears in more than a first threshold number of host pairs within the first update period, and a first historical number of host pairs is smaller than the first threshold number by a first factor value; and
 20. (2) the host appears in more than a second threshold number of host pairs within the second update period, and a second historical number of host pairs is smaller than the second threshold number by a second factor value.

1 2. (Previously presented) The method of claim 1 wherein the first
2 threshold number and the first factor value are adjustable.

1 3. (Previously presented) The method of claim 2 wherein the first data
2 structure is a current time-slice connection table and host-pair connection records
3 are added to the current time slice connection table.

1 4. (Previously presented) The method of claim 3, further comprising:
2 checking for ping scans at the end of the second update period; and
3 indicating hosts which produced more than the second threshold number
4 of new host pairs over the second update period.

1 5. (Cancelled)

1 6. (Previously presented) The method of claim 1 further comprising:
2 maintaining Address Resolution Protocol (ARP) packet statistics in the
3 first data structure and for sparse subnets tracking the number of generated ARP
4 requests that do not receive responses to detect scans on sparse sub-networks.

1 7. (Original) The method of claim 1 wherein the scanning attack is a ping
2 scanning attack.

1 8. (Currently amended) A computer implemented method of detecting port
2 scanning attacks, the method comprises:
3 retrieving from a first data structure stored on a computer readable
4 medium logged values of protocols and ports in host-pair connection records
5 added in the first data structure during a first update period;

6 determining the number of ports associated with a host over the first
7 update period based on the host-pair connection records in the first data structure;
8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update period; period, wherein aggregating host-pair
11 connection records involves partitioning hosts into groups that have similar
12 connection habits;
13 determining the number of ports associated with a host over the second
14 update period based on the host-pair connection records in the second data
15 structure; and
16 reporting a host associated with a port scan when at least one of the
17 following conditions is true:
18 (1) the number of ports associated with the host within the first update
19 period is greater than a first threshold number, and a first historical number of
20 ports associated with the host is smaller than the first threshold number by a first
21 factor value; and
22 (2) the number of ports associated with the host within the second update
23 period is greater than a second threshold number, and a second historical number
24 of ports associated with the host is smaller than the second threshold number by a
25 second factor value.

1 9. (Original) The method of claim 8 further comprising:
2 assigning a severity level to the port scan and reporting the severity level
3 of the port scan.

1 10. (Original) The method of claim 8 wherein the reported severity varies
2 as a function of the deviation from historical norm.

1 11. (Previously presented) The method of claim 8 further comprising:

2 determining from accessing data in the first data structure, statistics about
3 TCP reset (RST) packets and ICMP port-unreachable packets, to detect a spike in
4 the number of RST packets and ICMP port-unreachable packets to determine the
5 severity of a port scan event.

1 12. (Cancelled)

1 13. (Cancelled)

1 14. (Currently amended) A computer program product residing on a
2 computer readable medium for detecting scanning attacks, comprises instructions
3 for causing a computer to:

4 add host-pair connection records to a first data structure when a host
5 accesses another host during a first update period;

6 determine the number of new host pairs added to the first data structure
7 over the first update period;

8 aggregate host-pair connection records from the first data structure into a
9 second data structure which corresponds to a second update period that is greater
10 than the first update period; period, wherein aggregating host-pair connection
11 records involves partitioning hosts into groups that have similar connection
12 habits:

13 determine the number of new host pairs added to the second data structure
14 over the second update period; and

15 indicate a host as a scanner when at least one of the following conditions
16 is true:

17 (1) the host appears in more than a first threshold number of host pairs
18 within the first update period, and a first historical number of host pairs is smaller
19 than the first threshold number by a first factor value; and

20 (2) the host appears in more than a second threshold number of host pairs

21 within the second update period, and a second historical number of host pairs is
22 smaller than the second threshold number by a second factor value..

1 15. (Previously presented) The computer program product of claim 14
2 wherein the first threshold number and the first factor value are adjustable .

1 16. (Previously presented) The computer program product of claim 14
2 wherein the first data structure is a current time-slice connection table and host-
3 pair connection records are added to the current time slice connection table.

1 17. (Previously presented) The computer program product of claim 16,
2 further comprising instructions to:
3 check for ping scans at the end of a the second update period; and
4 indicate hosts which produced more than the second threshold number of
5 new host pairs over the second update period.

1 18. (Cancelled)

1 19. (Previously presented) The computer program product of claim 14
2 further comprising instructions to:
3 maintain Address Resolution Protocol (ARP) packet statistics in the first
4 data structure; and
5 track the number of generated ARP requests that do not receive responses
6 to detect scans on sparse sub-networks.

1 20. (Currently amended) A computer program product residing on a
2 computer readable medium for detecting port scanning attacks, the computer
3 program product comprises instructions for causing a processor to:

4 retrieve from a first data structure logged values of protocols and ports in
5 host-pair connection records in the first data structure during a first update period;
6 determine the number of ports associated with a host over the first update
7 period based on the host-pair connection records in the first data structure;

8 aggregate host-pair connection records from the first data structure into a
9 second data structure which corresponds to a second update period that is greater
10 than the first update period; period, wherein aggregating host-pair connection
records involves partitioning hosts into groups that have similar connection
habits;

13 determine the number of ports associated with a host over the second
14 update period based on the host-pair connection records in the second data
15 structure; and

16 report a host associated with a port scan when at least one of the following
17 conditions is true:

18 (1) the number of ports associated with the host within the first update
19 period is greater than a first threshold number, and a first historical number of
20 ports associated with the host is smaller than the first threshold number by a first
21 factor value; and

22 (2) the number of ports associated with the host within the second update
23 period is greater than a second threshold number, and a second historical number
24 of ports associated with the host is smaller than the second threshold number by a
25 second factor value.

1 21. (Original) The computer program product of claim 20 further
2 comprising instructions to:

3 assign a severity level to the port scan and report the severity level of the
4 port scan.

1 22. (Original) The computer program product of claim 21 wherein the
2 reported severity varies as a function of the deviation from historical norm.

1 23. (Previously presented) The computer program product of claim 21
2 further comprising instructions to:
3 determine from the first data structure statistics about TCP reset (RST)
4 packets and ICMP port-unreachable packets to detect a spike in the number of
5 RST packets and ICMP port-unreachable packets to determine the severity of a
6 port scan event.

1 24. (Currently amended) Apparatus comprising:
2 circuitry for detecting scanning attacks, comprising:
3 circuitry to add host-pair connection records to a first data structure when
4 a host accesses another host during a first update period;
5 circuitry to determine the number of new host pairs added to the first data
6 structure over a first update period;
7 circuitry to aggregate host-pair connection records from the first data
8 structure into a second data structure which corresponds to a second update period
9 that is greater than the first update period; period, wherein aggregating host-pair
10 connection records involves partitioning hosts into groups that have similar
11 connection habits;
12 circuitry to determine the number of new host pairs added to the second
13 data structure over the second update period; and
14 circuitry to indicate a host as a scanner when at least one of the following
15 conditions is true:
16 (1) the host appears in more than a first threshold number of host pairs
17 within the first update period, and a first historical number of host pairs is smaller
18 than the first threshold number by a first factor value; and
19 (2) the host appears in more than a second threshold number of host pairs

20 within the second update period, and a second historical number of host pairs is
21 smaller than the second threshold number by a second factor value.

1 25. (Previously presented) The apparatus of claim 24 wherein the first
2 threshold number and the first factor value are adjustable.

1 26. (Previously presented) The apparatus of claim 24 wherein the first data
2 structure is a current time-slice connection table and host-pair connection records
3 are added to the current time slice connection table.

1 27. (Previously presented) The apparatus of claim 24, further comprising:
2 circuitry to check for ping scans at the end of a second update period; and
3 circuitry to indicate hosts which produced more than the second threshold
4 number of new host pairs over the second update period.

1 28. (Currently amended) Apparatus comprising:
2 a processing device; and
3 a computer readable medium tangible embodying a computer program
4 product for detecting scanning attacks, the computer program product comprising
5 instructions for causing the processing device to:
6 add host-pair connection records to a first data structure when a host
7 accesses another host during a first update period;
8 determine the number of new host pairs added to the first data structure
9 over the first update period;
10 aggregate host-pair connection records from the first data structure into a
11 second data structure which corresponds to a second update period that is greater
12 than the first update period; period, wherein aggregating host-pair connection
13 records involves partitioning hosts into groups that have similar connection
14 habits:

15 determine the number of new host pairs added to the second data structure
16 over the second update period; and

17 indicate a host as a scanner when at least one of the following conditions
18 is true:

19 (1) the host appears in more than a first threshold number of host pairs
20 within the first update period, and a first historical number of host pairs is smaller
21 than the first threshold number by a first factor value; and

22 (2) the host appears in more than a second threshold number of host pairs
23 within the second update period, and a second historical number of host pairs is
24 smaller than the second threshold number by a second factor value..

1 29. (Previously presented) The apparatus of claim 28 wherein the first
2 threshold number and the first factor value are adjustable.

1 30. (Previously presented) The apparatus of claim 28 wherein the first data
2 structure is a current time-slice connection table and host-pair connection records
3 are added to the current time slice connection table.

1 31. (Previously presented) The apparatus of claim 28, wherein the
2 computer program product further comprises instructions to:
3 check for ping scans at the end of a second update period; and
4 indicate hosts which produced more than second threshold number of new
5 host pairs over the second update period.

1 32. (Cancelled)

1 33. (Currently amended) Apparatus comprising:
2 a processing device;

3 a computer readable medium tangibly embodying a computer program

4 product for detecting port scanning attacks, the computer program product

5 comprises instructions for causing a processor to:

6 retrieve from a first data structure logged values of protocols and ports in
7 host-pair connection records in the first data structure during a first update period;

8 determine the number of ports associated with a host over the first update
9 period based on the host-pair connection records in the first data structure;

10 aggregate host-pair connection records from the first data structure into a
11 second data structure which corresponds to a second update period that is greater
12 than the first update period; ~~period, wherein aggregating host-pair connection~~
13 ~~records involves partitioning hosts into groups that have similar connection~~
14 ~~habits;~~

15 determine the number of ports associated with a host over the second
16 update period based on the host-pair connection records in the second data
17 structure; and

18 report a host associated with a port scan when at least one of the following
19 conditions is true:

20 (1) the number of ports associated with the host within the first update
21 period is greater than a first threshold number, and a first historical number of
22 ports associated with the host is smaller than the first threshold number by a first
23 factor value; and

24 (2) the number of ports associated with the host within the second update
25 period is greater than a second threshold number, and a second historical number
26 of ports associated with the host is smaller than the second threshold number by a
27 second factor value.

1 34. (Original) The apparatus of claim 33 further comprising instructions

2 to:

3 assign a severity level to the port scan and report the severity level of the
4 port scan.

1 35. (Previously presented) The apparatus of claim 34 wherein the reported
2 severity varies as a function of the deviation from a historical norm.

1 36. (Previously presented) The apparatus of claim 34 further comprising
2 instructions to:

3 determine from the first data structure statistics about TCP reset (RST)
4 packets and ICMP port-unreachable packets to detect a spike in the number of
5 RST packets and ICMP port-unreachable packets to determine the severity of a
6 port scan event.

1 37. (Currently amended) A computer implemented method of detecting
2 scanning attacks, comprises:

3 adding host-pair connection records to a first data structure stored on a
4 computer readable medium when a host accesses another host during a first
5 update period;

6 determining the number of new host pairs added to the first data structure
7 over the first update period;

8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update period; period, wherein aggregating host-pair
11 connection records involves partitioning hosts into groups that have similar
12 connection habits;

13 determining the number of new host pairs added to the second data
14 structure over the second update period; and

15 indicating a host as a scanner when the host appears in more than a first
16 threshold number of host pairs within the first update period, and a first historical

17 number of host pairs is smaller than the first threshold number by a first factor
18 value.

1 38. (Currently amended) A computer implemented method of detecting
2 scanning attacks, comprises:

3 adding host-pair connection records to a first data structure stored on a
4 computer readable medium when a host accesses another host during a first
5 update period;

6 determining the number of new host pairs added to the first data structure
7 over the first update period;

8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update ~~period; period, wherein aggregating host-pair~~
11 connection records involves partitioning hosts into groups that have similar
12 connection habits;

13 determining the number of new host pairs added to the second data
14 structure over the second update period; and

15 indicating a host as a scanner when the host appears in more than a second
16 threshold number of host pairs within the second update period, and a second
17 historical number of host pairs is smaller than the second threshold number by a
18 second factor value.

1 39. (Currently amended) A computer implemented method of detecting
2 port scanning attacks, the method comprises:

3 retrieving from a first data structure stored on a computer readable
4 medium logged values of protocols and ports in host-pair connection records
5 added in the first data structure during a first update period;

6 determining the number of ports associated with a host over the first
7 update period based on the host-pair connection records in the first data structure;

8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update period; period, wherein aggregating host-pair
11 connection records involves partitioning hosts into groups that have similar
12 connection habits;
13 determining the number of ports associated with a host over the second
14 update period based on the host-pair connection records in the second data
15 structure; and
16 reporting a host associated with a port scan when the number of ports
17 associated with the host within the first update period is greater than a first
18 threshold number, and a first historical number of ports associated with the host is
19 smaller than the first threshold number by a first factor value.

1 40. (Currently amended) A computer implemented method of detecting
2 port scanning attacks, the method comprises:
3 retrieving from a first data structure stored on a computer readable
4 medium logged values of protocols and ports in host-pair connection records
5 added in the first data structure during a first update period;
6 determining the number of ports associated with a host over the first
7 update period based on the host-pair connection records in the first data structure;
8 aggregating host-pair connection records from the first data structure into
9 a second data structure which corresponds to a second update period that is
10 greater than the first update period; period, wherein aggregating host-pair
11 connection records involves partitioning hosts into groups that have similar
12 connection habits;
13 determining the number of ports associated with a host over the second
14 update period based on the host-pair connection records in the second data
15 structure; and
16 reporting a host associated with a port scan when the number of ports

17 associated with the host within the second update period is greater than a second
18 threshold number, and a second historical number of ports associated with the
19 host is smaller than the second threshold number by a second factor value.